UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/591,205	08/31/2006	Graham Richard Wyatt	06-707	6055

20306 7590 01/04/2012

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER	
AVERY, JEREMIAH L	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
01/04/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/591,205	WYATT ET AL.	
	Examiner	Art Unit	
	JEREMIAH AVERY	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 June 2011*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-5,7-10,12-16 and 22-25* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☐ Claim(s) _____ is/are rejected.

8)☒ Claim(s) *1-5,7-10,12-16 and 22-25* is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *31 August 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

I. Claims 17-21 were cancelled in a preliminary amendment.

II. Claims 6 and 11 have been cancelled.

III. Claim 25 has been added.

IV. Claims 1-5, 7-10, 12-16 and 22-25 have been examined.

V. Responses to Applicant's remarks have been given.

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 06/30/11 has been entered.

Response to Arguments

2. The objection to claim 7 has been withdrawn due to Applicant's amendment to said claim.

3. Due to the Applicant's arguments being persuasive, as well as the amendments made to independent claim 1; thus the 35 U.S.C. 112, second paragraph rejection of claims 15 and 16 is hereby withdrawn.

4. With regards to the Applicant's arguments pertaining to that Patton does not address the claimed features pertaining to dealing with "malicious code", the Examiner upholds that Walsh discloses such matters via column 9, lines 13-52, "Once the

computer is infected with the macro virus, each computer file that you save is automatically infected with the macro virus" and "A macro virus uses the macro programming language of an executable program to distribute the macro virus to data files on a computer system".

5. With regards to the Applicant's arguments pertaining to a "data diode", as it is known in the art, data diodes serve as connections between two or more networks of differing security classifications. Thus, Patton's disclosure via page 3, paragraph 31 and page 4, paragraph 40, "while authorized internal engineers 120 can have access to all global export DPs 118 on web site 124, the global engineers 122 are preferably limited to being able to access only global export issued DPs 118 that have been designated or assigned to the authorized global engineer 122 on web site 124" provides support for limiting the flow and access of particular data across different boundaries.

Claim Objections

6. Claim 12 is objected to because of the following informalities: claim 12 has a dependency to cancelled claim 11. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claim 25 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 25 states that "the at least one of a firewall and a data diode is a data diode and in which the second at least one of a firewall and a data diode

is a data diode". Claim 25 states that only the "data diode" is present out of the two options. Thus, it is unclear as to why "a firewall" was also provided as an option when claim 25 is interpreted to only encompass the "data diode".

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1, 2, 4, 5, 7-10, 12-14, 16 and 22-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent Application Publication No. US 2003/0145017 to Patton et al., hereinafter Patton and further in view of United States Patent No. United States Patent No. 7,624,277 to Simard et al., hereinafter Simard and further in view of United States Patent No. 5,956,481 to Walsh et al., hereinafter Walsh.

8. Regarding claims 1, 22, 23 and 24, Patton teaches a method, an apparatus, a computer chipset and a non-transitory computer readable medium having program code record thereon for communicating an electronic document between a first and second

security domain[[s]], each security domain comprising a network having a common level of resilience to security threats, the method comprising the steps of:

receiving, in the first security domain (page 3, paragraph 29, "internal source" and "United States"), a request to transmit to the second security domain (page 3, paragraph 29, "external sources" and "out of the United States or to foreign persons, whether in the United States or abroad") a first electronic document in a first data format capable of supporting *one or more* covert security threats (page 3, paragraph 29);

forwarding the first electronic document via *at least one of* a firewall and a data diode to a computerized format converter (page 3, paragraph 31 and page 4, paragraph 40);

applying the computerized format converter to the first electronic document whereby to create a second document in a second data format incapable of supporting the one or more security threats, responsive to the content of the first document (page 3, paragraph 30, "remove restricted information, technical data and proprietary information from a master document" and paragraph 32, page 4, paragraph 37, "the draft DP 108 is in a word processing file format such as Microsoft Word, Corel WordPerfect or any other suitable word processing format. The draft DP 108 can be converted using the sanitization application and the process described in greater detail below, to a 'sanitized' draft DP 110 and a 'sanitized' draft DP log 112." and paragraph 39, "issued DP 114 is preferably converted into a HTML format or a read-only, portable file format, e.g. PDF" and page 5, paragraph 47, "the author 102 can also perform character or text searches, which are described in steps 318-320, on the 'sanitized' draft

DP 110 in its portable or read-only format, e.g. in its PDF format, rather than on the draft DP 108 in its word processing format, e.g. in its Word format");

forwarding the second document in place of the first document to the second security domain (page 3, paragraph 31, "After making a determination to provide specific content included within the log file to an external or global source and taking some additional steps to ensure that appropriate security and authorization procedures have been followed, the specific content included within the log file can be transferred to the external or global source following the more restrictive U.S. Government export control license or company or organizational legal arrangements").

9. Patton teaches the claimed invention, as cited above. However, Patton does not teach the claim feature pertaining to "said security threats comprising presence in the first document of malicious code". Walsh teaches said feature, as cited below.

10. Regarding claims 1, 22, 23 and 24, Walsh teaches said security threats comprising presence in the first document of malicious code (Figure 2, elements 204 and 208, Figure 3, elements 302 and 304, Figure 4C and Figure 5B, column 7, lines 3-10, column 9, lines 13-52, "Once the computer is infected with the macro virus, each computer file that you save is automatically infected with the macro virus" and "A macro virus uses the macro programming language of an executable program to distribute the macro virus to data files on a computer system").

11. The motivation to combine would be to provide "a system for protecting a computer from infection by a virus that attacks data files of an executable program" (*Walsh* – column 2, lines 62-64).

12. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Walsh with the teachings of Patton in order to "protect against an unauthorized loading of a virus component, such as macro code, that can result in damage to data file content and to computer storage" (Walsh – column 2, lines 65-67 and column 3, lines 1-4).

13. Patton and Walsh teach the claimed invention, as cited above. However, Patton and Walsh do not teach the claim language pertaining to "wherein creating said second document comprises adding *at least one of* entropy and randomness to at least one characteristic of the representation of the first document". Simard teaches said claim language, as cited below.

14. Regarding claims 1, 22, 23 and 24, Simard teaches wherein creating said second document comprises adding *at least one of* entropy and randomness to at least one characteristic of the representation of the first document (column 6, lines 3-11, "generate a random character string image" and column 7, lines 36-52, "generates each image using a random set of characters").

15. The motivation to combine to prevent "a script from successfully running a repetitive task that is supposed to be performed by a human" (*Simard* – column 3, lines 5-7).

16. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Simard with the teachings of Patton and Walsh to provide a methodology that "yields significant reductions in

spam, software piracy, and operating costs and yields significant improvements in security" (*Simard* – column 3, lines 18-20).

17. Regarding claim 2, Patton teaches in which forwarding of the second document is conditional upon user sanction (page 4, paragraph 39, "Once the draft DP 108, the sanitized draft DP 110 and the sanitized draft DP log 112 have been approved by approvers 106, the draft DP 108 is then converted into an issued DP 114 that operates as a master document, a global export issued DP log 116 and a global export issued DP 118.").

18. Regarding claim 4, Patton teaches in which the second document is forwarded to the second security domain via a second *at least one of* a firewall and a data diode (page 3, paragraph 31 and page 4, paragraph 40).

19. Regarding claim 5, Patton teaches in which the step of creating the second document comprises performing a transformation to the first document which modifies the underlying data format of the document whilst preserving the visible informational content (page 4, paragraph 39, "issued DP 114 is preferably converted into a HTML format or a read-only, portable file format, e.g. PDF" and page 5, paragraph 47, "the author 102 can also perform character or text searches, which are described in steps 318-320, on the 'sanitized' draft DP 110 in its portable or read-only format, e.g. in its PDF format, rather than on the draft DP 108 in its word processing format, e.g. in its Word format").

20. Regarding claim 7, Patton teaches in which the at least one characteristic comprises *at least one of* colour and spacing (page 6, paragraph 52, "the collapsing of any spaces" and paragraph 55 and page 7, remainder of paragraph 57).

21. Patton anand Walsh teaches the claimed invention, as cited above. However, Patton and Walsh do not teach the claim language pertaining to "in which the step of creating the second document comprises applying a lossy compression method". Simard teaches said claim language, as cited below.

22. Regarding claim 8, Simard teaches in which the step of creating the second document comprises applying a lossy compression method (column 12, lines 29-34).

23. The motivation to combine would be "because the lossy compression yields even smaller images and additional security" (*Simard* - column 12, lines 31-34).

24. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Simard with the teachings of Patton and Walsh to render the data in a manner "that a human can easily read but that is hard for a computer to read" (*Simard* – column 12, lines 45-57).

25. Regarding claim 9, Patton teaches comprising the step of: conveying the second document to a user sanction function for review and sanction prior to sending the second document to the second security domain (page 3, paragraph 31, "The log file can be viewed by authorized internal users to confirm what information has been removed from the document or to determine if specific contents of the log file can be provided to an external source under more restrictive export control licenses or appropriate legal arrangements.").

26. Regarding claim 10, Patton teaches in which review and sanction comprises sanction by a human user (page 3, paragraph 35, "In other words, the sanitization application can be downloaded to the authorized user's computer from another computer over a network connection or an Internet connection and can then be operated without the network connection. The user is able to use the sanitization application without a network connection and is able to store the master documents, sanitized documents, document log files and related information and documents in a database." and page 4, remainder of paragraph 35 and paragraph 39, "The draft DP 108, the sanitized draft DP 110 and the sanitized DP log 112 can be reviewed by reviewers 104, which can include author 102, and then approved by approvers 106, which can include author 102 and reviewers 104).

27. Patton and Simard teach the claimed invention, as cited above. However, they do not teach the claim features of claim 12 pertaining to "malicious code" and examples thereof. Walsh discloses said features, as cited below.

28. Regarding claim 12, Walsh teaches in which the malicious code comprises *at least one of* a computer virus, a worm, a Trojan horse, a back door attack, a BIOS attack, a microcode malware attack, a social engineering attack, and buffer overflow attack (Figure 2, elements 204 and 208, Figure 3, elements 302 and 304, Figure 4C and Figure 5B, column 7, lines 3-10, column 9, lines 13-52, "Once the computer is infected with the macro virus, each computer file that you save is automatically infected with the macro virus" and "A macro virus uses the macro programming language of an

executable program to distribute the macro virus to data files on a computer system", column 10, lines 7-34, column 11, lines 16-28, column 12, lines 26-37 and 53-65).

29. The motivation to combine would be to provide "a system for protecting a computer from infection by a virus that attacks data files of an executable program" (*Walsh* – column 2, lines 62-64).

30. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Walsh with the teachings of Patton and Simard in order to "protect against an unauthorized loading of a virus component, such as macro code, that can result in damage to data file content and to computer storage" (Walsh – column 2, lines 65-67 and column 3, lines 1-4).

31. Patton and Simard teach the claimed invention, as cited above. However, they do not teach the claim features of claim 13 pertaining to "in which one or more security threats comprises data steganographically concealed within the first document". Walsh teaches said feature, as cited below.

32. Regarding claim 13, Walsh teaches in which the *one or more* security threats comprises data steganographically concealed within the first document (column 2, lines 4-6, "macro virus could attack a document by inserting a copy of itself into the data file" and column 9, lines 13-52, "Once the computer is infected with the macro virus, each computer file that you save is automatically infected with the macro virus" and "A macro virus uses the macro programming language of an executable program to distribute the macro virus to data files on a computer system").

33. The motivation to combine would be to provide "a system for protecting a computer from infection by a virus that attacks data files of an executable program" (*Walsh* – column 2, lines 62-64).

34. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Walsh with the teachings of Patton and Simard in order to "protect against an unauthorized loading of a virus component, such as macro code, that can result in damage to data file content and to computer storage" (Walsh – column 2, lines 65-67 and column 3, lines 1-4).

35. Regarding claim 14, Patton teaches in which the first security domain and second security domain are rated at different security levels (page 3, paragraphs 29-31, "the master document, when viewed by internal or company users, is identical to the original or master document, except that the information designated for removal from the original or master document is distinguished from the remaining text and/or graphics. In contrast, when viewed by an external or global source, the sanitized document does not include any information designated for removal from the original or master document").

36. Regarding claim 16, Patton teaches in which the first security domain is a higher-level security domain than the second security domain (page 3, paragraph 29, "internal source" and "United States", "external sources" and "out of the United States or to foreign persons, whether in the United States or abroad" and paragraph 31).

[Wherein the claimed "first security domain" is interpreted by the Examiner to pertain to Patton's disclosure of an "internal source" and "the United

States" with regards to certain information not being able to be sent outside of the United States. The claimed "second security domain" pertains to Patton's disclosure of "external sources" and to areas "out of the United States".]

37. (New) Regarding claim 25, Patton teaches in which the *at least one of* a firewall and a data diode is a data diode and in which the second at least one of a firewall and a data diode is a data diode (page 3, paragraph 31 and page 4, paragraph 40).

38. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Patton, Walsh and Simard as applied to claim 1 above, and further in view of United States Patent No. 5,787,175 to Carter, hereinafter Carter.

39. Patton, Walsh and Simard teach the claimed invention, as cited above. However, Patton and Simard do not teach the claim language within claim 3 pertaining to "in which the second document is digitally signed by a sanctioning user". Carter teaches said claim language, as cited below.

40. Regarding claim 3, Carter teaches in which the second document is digitally signed by a sanctioning user (column 17, lines 28-47, "Collaborative signatures control the attribution of a given version of the work group document 90 to one or more members of the collaborative group").

41. The motivation to combine would be "to provide such a method and apparatus which limit access to work group documents to those people who are expected to contribute directly to the document" (*Carter* - column 5, lines 25-28).

42. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Carter with the teachings of Patton, Walsh and Simard "to provide such a method and apparatus which permit any given member of the work group to independently change the cryptographic method used for key generation in order to foil unauthorized decryption attempts, without preventing authorized access to the document" (*Carter* – column 5, lines 62-67).

43. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Patton, Walsh and Simard as applied to claim 1 above, and further in view of United States Patent No. 6,304,973 to Williams, hereinafter Williams.

44. Patton, Walsh and Simard teach the claimed invention, as cited above. However, Patton and Simard do not teach the claim language pertaining to "the first security domain is a lower-level security domain than the second security domain". Williams teaches said claim language, as cited below.

45. Regarding claim 15, Williams teaches in which the first security domain is a lower-level security domain than the second security domain (Figure 6, column 13, lines 10-21, "a Multi-Level Secure computer that is capable of simultaneously processing a range of Secret to Top Secret" and lines 25-37 and column 14, lines 7-9).

46. The motivation to combine would be "to provide a security device that prevents unauthorized third parties from gaining access to a host. It is another object of the invention to provide a multi-level secure network having a security device coupled between each host and the network medium" (*Williams* – column 4, lines 31-35).

47. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Williams with the teachings of Patton, Walsh and Simard so that the "network prevents unauthorized users from gaining access to sensitive information" (*Williams* - column 4, lines 41 and 42).

Conclusion

48. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

49. The following United States Patents are cited to further show the state of the art with respect to secure distribution of messages within a network environment:

United States Patent No. 7,130,885 to Chandra et al., which is cited to show methods and apparatus providing electronic messages that are linked and aggregated.

United States Patent No. 6,216,231 to Stubblebine, which is cited to show specifying security protocols and policy constraints in distributed systems.

United States Patent No. 7,216,043 to Ransom et al., which is cited to show a push communications architecture for intelligent electronic devices.

50. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEREMIAH AVERY whose telephone number is (571)272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

51. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

52. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jeremiah Avery/
Examiner, Art Unit 2431
/NATHAN FLYNN/
Supervisory Patent Examiner, Art Unit 2431